UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/085,927	02/27/2002	Gregory Eugene Perkins	100201141-1	1153

7590   04/06/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER
BAYARD, DJENANE M

ART UNIT	PAPER NUMBER
2141	

DATE MAILED: 04/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/085,927	PERKINS ET AL.
	Examiner	Art Unit
	Djenane M. Bayard	2141

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 January 2006*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   This is in response to amendment filed 1/19/06 in which claims 1-25 are pending.

Response to Arguments

2.   Applicant's arguments have been fully considered but they are not persuasive.

Therefore, the rejection stand as stated in the previous office action dated 10/19/05.

As per claim 1, 5, 9, 17 and 24, Applicant argues that Sampson fails to teach "providing

an interface having instructions to send association data." However, Sampson teaches " a client

executing a browser and communicates with one or more access servers." As per applicant

specification, " Interface: the junction between a user and a computer program providing

commands or menus through which a user communicates with the program... the interface can

be a web page from a website or a programmatic interface from a web service (See paragraph

[0018]]). It is well known to one with ordinary skill in the art that a web browser is a

programmatic interface that serves as your front end to the Web on the Internet. As per applicant

specification "association data" is a "data associating a user with a session" (See paragraph

[0027]). Sampson clearly teaches wherein the browser is sending cookie to a protected server

(See col. 7, lines 64-65) and wherein the information in the cookie is used to verify that the user

is authorized to access the resource (See col. 8, lines 1-2).

Applicant argues Sampson fails to teach " identifying an identity service using the

association data, the identity service managing resource data". As per applicant' specification,

Identity server represents any programming capable of receiving and responding to request made

by application service for the network address and credentials needed to locate and access

resource device   Client 16 may access identity service 36 as well to provide needed information. Identity Server 36 is also responsible for managing identity table 38. Identity table 38 represents a logical memory area accessible by identity table interface 40 and used to contain identity data. Identity data is data used to locate and access a particular resource 30. Identity data will include the network address or URL for the resource 30 or - more generally - any means by which the network address or URL for resource 30 can be obtained. Identity data also includes credentials for accessing the resource. Credential may include a user name and password pair, an encryption/decryption key, and/or any other data used to access secure identity service includes identity server, identity table, identity table interface." (See paragraph 0026]). Sampson et al clearly teaches wherein the session manger takes the session ID and performs checks on it (See col. 13, lines 5-15) and upon receipt of the status code value from the session manager the electronic document is created and sent to the client (See col. 13, lines 40-67). Furthermore, Sampson teaches wherein the client requests a protected resource from protected server (See col. 14, lines 25-26).

Applicant argues that Sampson fails to teach "locating the resource using the resource data." As per applicant's specification, "resource data may include the network address and a description of each resource. It may also include any credentials such as a username and password needed to access the resource" (See paragraph [0031]). Sampson clearly teaches wherein based on the session ID, the client can access resources on the protected server (See col. 13 and col. 14).

Applicant's arguments do not comply with 37 CFR 1.111(c) because they do not clearly

point out the patentable novelty which he or she thinks the claims present in view of the state of

the art disclosed by the references cited or the objections made.

As per claim 6, Applicant argues Sampson et al fails to teach " the acts of providing a

web page, requesting a web bug, and saving the cookie". However, Sampson et al clearly

teaches a system that enables Users to login to the system once, and thereafter access one or

more Resources during an authenticated session. Users may log in either with a digital

certificate or by opening a login page URL with a web browser and entering a name and

password. Access Server 106 stores a login page, Authentication Client Module and Access

Menu Module. The Authentication Client Module authenticates a user by verifying the name

and password with the Registry Server 108. If the name and password are correct, the

Authentication Client Module reads the user's roles from the Registry Server 108. It then

encrypts and sends this information in a "cookie" to the user's browser. A "cookie" is a packet

of data sent by web servers to web browsers. Each cookie is saved by browser 100 until the

cookie expires. Cookies received from a web server in a specific domain are returned to web

servers in that same domain during open URL requests. A cookie returned by the

Authentication Client Module is required for access to resources protected by the system (See

col. 7 and col. 10).

Furthermore, Applicant argues Sampson fails to teach identifying other entries in the

association table containing the cookie, identifying from those entries an entry containing URL

for an identification service. However, Sampson et al teaches wherein "Client 100 obtains a

resource that is protected by Protected Server 104A, and in the course of obtaining it, Client 100

is authenticated in the system. Runtime 406A notifies Session Manager 420A that it is

conducting a session with Client 100. A new set of session information is created by Session

Manager 420A. Session Manager 420A stores the current time in the Last Access Time value

of the set of session information that is associated with the current session between Clients

100 and Runtime 406A. Session Manager 420A notifies Session Manager 420B to update the

Last Access time value in the replicated session information that it stores for the same session.

Client 100 then requests a protected resource from Protected Server 104B. Runtime 406B

updates the Last Access Time value, and provides it to Session Manager 420A, which also

updates its copy of the Last Access Time. Assume that Client 100 actively works with

resources managed by Protected Server 104B for more than 15 minutes, and then returns to

Access Server 104A to obtain one of its protected resources. Since the Last Access Time value

is updated by Session Manager 420B each time Client 100 interacts with Access Server 104B,

Session Manager 420A determines that Client 100 is active and may interact with Protected

Server 104A to access its resources. However, if the Session Managers did not communicate

with one another to update session information, Session Manager 420A would determine that

Client 100 last contacted it more than 15 minutes ago, and an Idle Timeout error would

occur. Client 100 would be required to re-authenticate itself before Access Server 104B could

grant access to its protected resources. Alternatively, in this example Session Manager 420B

could contact Session Manager 420A and obtain the Last Access Time value for the current

session only when the Client 100 contacts Session Manager 420B. However, if the link

between Session Manager 420A and Session Manager 420B was busy, down, or unavailable,

Session Manager 420B would be unable to obtain such information." (See col. 14, lines 10-50)

Sampson et al teaches wherein identifying other entries in the association table containing the

cookie, identifying from those entries an entry containing URL for an identification service.

As per claim 20, Applicant argues that Samson et al fails to teach "a system that includes

an identify service operable to manage resource data, and an association server operable to

receive association data containing a client identifier and a session identifier, save the association

data in an association table, and receive queries for the association table". However, Sampson et

al clearly teaches wherein "the message request validation of a session between the client and the

protected server, and contains information including a session identifier value (Session ID)... the

Session manager object takes the Session Id and performs checks on it... The Session manager

object checks to determine whether the Session ID is recognized or known, by searching a local

hash table of the Session Manager object to find the Session ID" (See col. 13, lines 5-19 and col.

11, lines 1-16). Furthermore, Applicant argues that Sampson et al fails to teach an association

module operable to query, supplying a session identifier, the association service in order to

identify the identity service". However, Sampson et al clearly teaches wherein a session Id is

supplied in order to access protected resources. The Session Manager checks to determine

whether the Session ID is recognized or known, and based on the status code of the check the

client will be permitted or not access the requested resource (See col. 13 and 14).

As per claim 7, 19 and 22, Applicant argues Sampson et al fails to teach " a method

"querying the association service to identify an identity service with which the user is registered

providing an URL for the generated web page. However, Sampson et al clearly teaches wherein

each session between a client and a server is represented by a set of session information. The

session information preferably comprises: an initial session identifier value; an initial access time

value; a last access time value; a user identifier value or key ... (See col. 10, lines 39-46).

Furthermore, Sampson et al teaches wherein the client accesses protected resources based on the

status code of the session ID after it has been searched and checked against the hash table of the

session manager. Furthermore, Sampson et al teaches wherein the client will have access to the

requested resources after completion of the check based on the value of the status code (See col.

13, lines 5-53).

Furthermore, Applicant argues that Lu is not relevant to claim 7. However, Lu teaches

locating and accessing a document management service using the resource data (wherein the

visitor makes a web page request by typing in a URL into a browser to a web server (See page 4,

paragraph [0064])); providing additional content for the web page for displaying controls for

selecting a document managed by the document management service (the web site is constructed

using a html or JavaScript code including the original web page code, data mining code, and

additional cookie processing code (See page 4, paragraph [0064]); producing a document

according to selections made through the web page (the web page loads via the browser at the

client (see page 4, paragraph [0064-0066]).

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed
> in the United States before the invention by the applicant for patent or (2) a patent granted on an application for
> patent by another filed in the United States before the invention by the applicant for patent, except that an

international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4.   Claims 1-6 and 9-14, 17 and 20-21 are rejected under 35 U.S.C. 102(e) as being

anticipated by U.S. Patent No. 6490624 to Sampson et al.

a.   As per claims 1, 9 and 24, Sampson et al teaches in a computer network, a method for

locating a resource, comprising: providing an interface having instructions to send association

data (See col. 9, lines 4-5); Furthermore, Sampson et al teaches identifying an identity service

using the association data, the identity service managing resource data (See col. 13, lines 5-67);

and locating the resource using the resource data (See col. 14, lines 25-35).

b.   As per claim 2 and 10, Sampson et al teaches the claimed invention as described above.

Furthermore, Sampson et al teaches performing a specified task utilizing the resource (See col. 7,

lines 5-21).

c.   As per claim 3 and 11, Sampson et al teaches the claimed invention as described above.

Furthermore, Sampson et al fails to teach wherein the association data includes a client identifier

and a session identifier associated with the interface, and wherein the act of identifying

comprises: providing the session identifier associated with the interface, identifying the client

identifier included in the association data; identifying other association data containing that client

identifier; and acquiring at least a portion of the session identifier included in the other

association data (See col. 10, lines 40-67).

e.   As per claims 5, 13 and 17, Sampson et al teaches a method for locating a resource for a

user, comprising: providing an interface having instructions to send association data to two or

more association services (See col. 9, lines 4-5); identifying from the two or more association

services, an association service with which the user has established a relationship (See col. 10,

lines 32-45); Furthermore, Sampson et al teaches identifying an identity service using the

association data sent to the identified association service (See cool. 13, lines 5-67), the identity

service managing resource data; and locating the resource using the resource data (See col. 14,

lines 25-35).

a.   As per claims 6 and 14, Sampson et al teaches providing a web page having instructions

to request a web bug; requesting the web bug sending a cookie and an URL for the web page;

saving the cookie and the URL for the web page as an entry in an association table (See col. 10,

lines 10-4); querying, providing the URL for the web page, the association table for the cookie in

the entry containing the URL; identifying other entries in the association table containing the

cookie; identifying from those entries an entry containing an URL for an identification service,

the identification service managing resource data; and locating the resource using the resource

data (See col. 14, lines 25-35).

f.   As per claims 20 and 21, Sampson et al teaches a system for locating a resource,

comprising: an identity service operable to manage resource data; an association server operable

to receive association data containing a client identifier and a session identifier, save the

association data in an association table, and receive queries for the association table (See col. 10,

lines 40-45); an association table interface in communication with the association server and

operable, according to a received query, to access from the association table a session identifier

for the identity service using a session identifier supplied with the query (See col. 11, lines 1-14

and col. 13, lines 1-18).); an association module operable to query, supplying a session identifier,

the association service in order to identify the identity service; an application operable to:

provide an interface having instructions to send association data to an association server, the

association data to contain a client identifier and a session identifier for the provided interface

(See 9, lines 52-67); Furthermore, Sampson teaches acquiring resource data from the identity

service identified by a query from the association module; and locate the resource using the

resource data (See col. 14, lines 25-35).

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

6.   Claims 4, 7-8, 15-16 and 18-19, 22 and 24-25 are rejected under 35 U.S.C. 103(a) as

being unpatentable over U.S. Patent No. 6490624 to Sampson et al in view of U.S Patent

Application No. 20040015580 to Lu et al.

a.   As per claim 4, Sampson et al teaches the claimed invention as described above.

However, Sampson et al fails to teaches wherein the act of providing comprises providing a web

page having instructions to request a web bug sending association data containing a cookie and

an URL for the web page; and wherein the act of identifying comprises: providing the URL to

identify the association data containing the cookie; identifying other association data containing

the cookie; and acquiring an URL for the identity service from the identified association data.

Lu et al teaches a system and method for generating and reporting cookie values at a

client node. Furthermore, Lu et al teaches providing a web page having instructions to request a

web bug sending association data containing a cookie and an URL for the web page (See page 4,

paragraph [0059]); and wherein the act of identifying comprises: providing the URL to identify

the association data containing the cookie; identifying other association data containing the

cookie; and acquiring an URL for the identity service from the identified association data (See

page 4, paragraph [0064]).

It would have been obvious to one with ordinary skill in the art at the time the invention

was made to incorporate providing a web page having instructions to request a web bug sending

association data containing a cookie and an URL for the web page; and wherein the act of

identifying comprises: providing the URL to identify the association data containing the cookie;

identifying other association data containing the cookie; and acquiring an URL for the identity

service from the identified association data as taught by Lu et al in the claimed invention of

Sampson et al in order to establish and process a cookie right on the client node without

additional interaction with the web tracking provider (See page 4, paragraph [0064]).

b.   As per claims 7, 15, 19, 22 and 24-25, Sampson et al teaches a method for producing an electronic document, comprising: generating, upon request from a user, a web page having content for requesting a web bug from an association service as well as content for displaying controls for selecting production options; querying the association service to identify an identity service with which the user is registered providing an URL for the generated web page; obtaining the user's resource data from the identified identity service (See col. 10, lines 40-45); However, Sampson et al fails to teach locating and accessing a document management service using the resource data; providing additional content for the web page for displaying controls for selecting a document managed by the document management service; and producing a document according to selections made through the web page.

Lu et al teaches locating and accessing a document management service using the resource data; providing additional content for the web page for displaying controls for selecting a document managed by the document management service; and producing a document according to selections made through the web page (See page 4, paragraph [0064]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate locating and accessing a document management service using the resource data; providing additional content for the web page for displaying controls for selecting a document managed by the document management service; and producing a document according to selections made through the web page as taught by Lu et al in the claimed invention of Sampson et al in order to establish and process a cookie right on the client node without additional interaction with the web tracking provider (See page 4, paragraph [0064]).

c.   As per claims 8 and 16, Sampson et al teaches wherein: the act of generating comprises

generating a web page having instructions to request a web bug sending, to the association

service association, data containing a cookie and an URL for the web page; the method further

comprises saving the association data as an entry in an association table; the act of querying

further comprises identifying the cookie in the saved entry using the provided the URL,

identifying other association data containing the identified cookie, and, from the other identified

association data, acquiring an URL for the identity service; and the act of obtaining the user's

resource data comprises obtaining the user's resource data from the identified identity service

using, at least in part, the acquired URL (See col. 9, lines 35-67).

d.   As per claim 18, Sampson et al teaches wherein: the application is further operable to

provide the interface in the form of a web page having instructions to send association data

containing a cookie and the URL for the provided web page; and the association module is

further operable to provide the URL and query the association service for an URL for the identity

service (See col. 9, lines 30-67).

Conclusion

7.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing

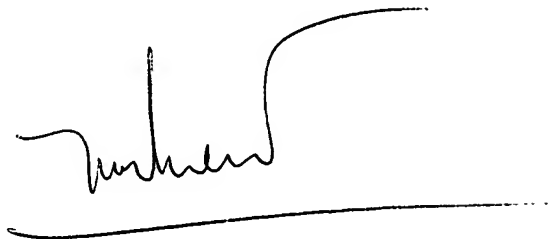date of this final action.

8.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Djenane M. Bayard whose telephone number is (571) 272-3878.

The examiner can normally be reached on Monday- Friday 5:30 AM- 3:00 PM..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Rupal Dharia can be reached on (571) 272-3880. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Djenane Bayard

Patent Examiner